bugcrowd

DATA SHEET

Red Team as a Service

Crowdsourced red teaming that simulates real attacks for stronger, real-world defense

Bugcrowd's Red Team as a Service (RTaaS) is the first-ever offering to bring the scale, agility, and rewards-driven impact of crowdsourcing to red teaming—by connecting customers to a global, elastic network of vetted operators for multiple types of engagements fully managed on the Bugcrowd Platform.

This radically new approach to red teaming combines traditional, blended, and continuous models, ensuring persistent, real-world attack simulations that can evolve to address emerging threats.

Unlike rigid, one-off engagements, RTaaS flows findings into existing DevSec processes. This will help you proactively identify and address vulnerabilities across people, processes, and technology—turning findings into action before adversaries exploit them.

Bugcrowd RTaaS

A radical new approach to proactive security

Breaches are costing companies an average of $4.84M* requiring organizations to need more than typical security efforts to stay ahead of persistent, advanced threats. Bugcrowd's RTaaS offers:

Real-world adversarial tactics

Bugcrowd RTaaS goes beyond traditional red team exercises by offering ongoing, adaptive testing. It uncovers evolving attack chains—just like real cybercriminals, hackers, and nation-state actors.

Scalable and flexible

Easily scale your engagement up or down by using Bugcrowd's global pool of vetted operators and multiple tier options (Assured, Blended, or Continuous) of red team operations to ensure fresh tactics and up-to-date skills.

Unified platform for every maturity stage

RTaaS works seamlessly with Bugcrowd's Pen Testing as a Service, Managed Bug Bounty, and Vulnerability Disclosure Programs, enabling organizations to address every stage of security maturity under a single platform—all while growing alongside evolving security needs.

Legacy Red Teams vs. Bugcrowd RTaaS

Traditional Red Teams	Bugcrowd RTaaS Subscription
Rigid, time-boxed engagements	✓ Flexible scheduling and continuous programs
Limited operator availability	✓ Global bench of vetted specialists across 350+ skills
Delayed reporting, minimal collaboration	✓ Real-time visibility and updates via the platform
Large, hard-to-digest final reports	✓ Actionable insights integrated into DevSec workflows
Hard to scale for new or shifting assets	✓ On-demand elasticity to adapt to emerging threats

*2024 Cost of a Data Breach Report by IBM Security

BUGCROWD

DATA SHEET

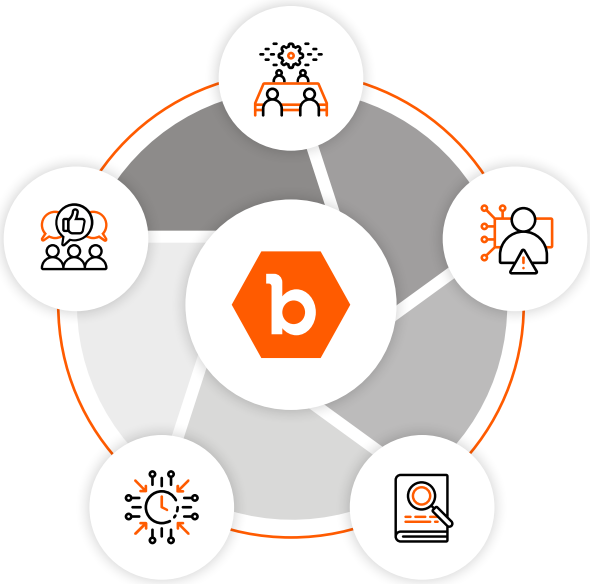
Bugcrowd RTaaS
How it works

Adversarial simulation

Skilled operators execute attack strategies aligned with real-world threats. The Bugcrowd team coordinates each step, ensuring methodology and goals are met.

Customizable engagement planning and launch

Work with Bugcrowd experts to set clear objectives and constraints, integrate threat intelligence, address compliance needs, and set organizational priorities.



Ongoing support and improvement

Access Bugcrowd's global intelligence and best practices, continuously updated based on thousands of customer engagements, to evolve your testing scope as your environment or threats change. This will ensure security improvements persist over time.

Real-time visibility and attack approval

Get real-time visibility and notifications to approve and refine attack paths on the fly using an interactive dashboard within the Bugcrowd Platform.

Comprehensive reporting and remediation

Detailed reports include adversarial tactics, attack chains, root-cause analysis, and actionable remediation guidance. These allow you to see long-term effects and meet compliance requirements.

Flexible engagement models for real-world impact

Bugcrowd offers three red teaming models designed for various maturity levels, compliance needs, or budget.

Assured Red Teaming

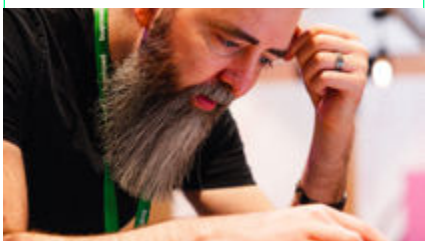
Fully managed, dedicated team

A dedicated team of expert operators is deployed for a set period, working closely with the client to meet specific security objectives. This traditional red team approach ensures deep collaboration, reliability, and an assessment of the organization's security posture. Each team is CrowdMatched to fit the unique needs of your organization.

Blended Red Teaming

Crowdsourced Ops Team
+ Assured team

A hybrid model that combines traditional red teaming with scalable, on-demand testing. Clients benefit from the collaborative efforts of highly skilled operators with initial phases conducted by a trusted group of vetted crowd operators. An Assured Red Team then takes over, ensuring a dynamic and adaptable security assessment.



Continuous Red Teaming

Ongoing, open-scope testing

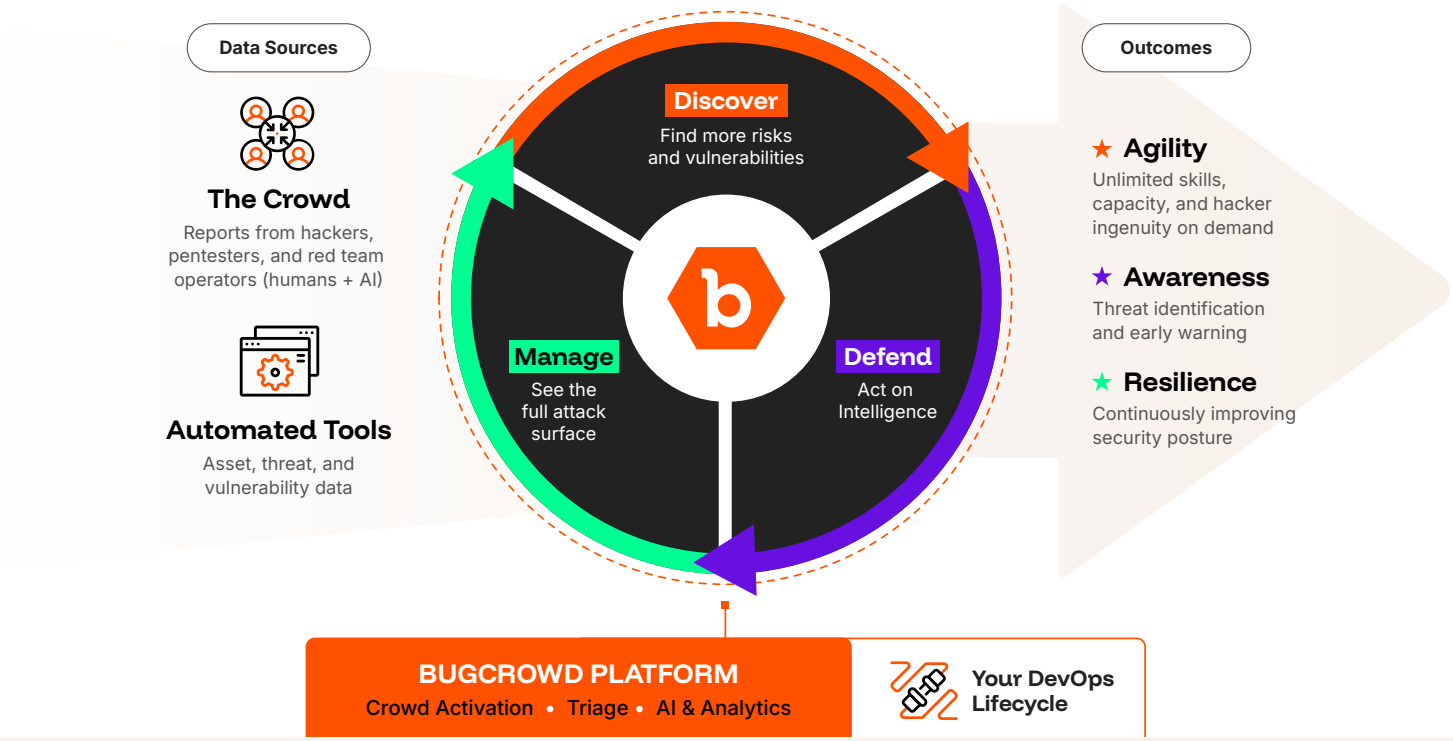
Ongoing security testing that adapts to evolving threats. Trusted teams of vetted experts rotate through ongoing assessments. These operations replicate real-world attacks helping organizations strengthen their defenses against the most realistic threats.

BUGCROWD

DATA SHEET

The Bugcrowd Platform

The Bugcrowd Platform helps customers defend themselves against cybersecurity attacks by connecting with trusted, skilled hackers to take back control of the attack surface. Our AI-powered platform for crowdsourced security is built on the industry's richest repository of data about vulnerabilities and hacker skill sets, activating the ideal hacker talent needed on demand, and bringing scalability and adaptability to address current and emerging threats.



Best Security ROI from the Crowd

We match you with trusted security researchers who are perfect for your needs and environment across hundreds of dimensions using machine learning.

Instant Focus on Critical Issues

Working as an extension of the platform, our global security engineering team rapidly validates and triages submissions, with P1s often handled within hours.

Contextual Intelligence for Best Results

We apply over a decade of knowledge accumulated from experience devising thousands of customer solutions to achieve your goals for better outcomes.

Continuous, Resilient Security for DevOps

The platform integrates workflows with your existing tools and processes to ensure that apps and APIs are continuously tested before they ship.

mastercard indeed credit karma Pinterest NASA ATLASSIAN

Unleash Human Creativity for Proactive Security

TRY BUGCROWD